UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,051	10/24/2003	Robert Derek La Gesse	08-1471-US	1539

20306 7590 10/27/2009

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
WU, JUNCHUN	
ART UNIT	PAPER NUMBER
2191	

MAIL DATE	DELIVERY MODE
10/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/693,051	LA GESSE ET AL.	
	Examiner	Art Unit	
	JUNCHUN WU	2191	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 9-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 9-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the amendment filed on June 19, 2009.

2. Claims 1-7, and 9-32 are pending in this application.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-5 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Bunger (U.S. Patent No. 6,944,859 B1 hereinafter Bunger), in view of Fordemwalt et al. (US Pub No. 20020147973 A1 hereinafter "Fordemwalt"), and further view of Palekar et al. (US Patent No. 6,941,465 B1 hereinafter "Palekar")

Per claim 1 (Currently amended)

Bunger discloses

- A method comprising: sending a device driver file and a first portion of network-specific data from a station to a host computing device (see col.9 lines 28-34 *"After opening the synchronization session, the client-handheld conduit file is transmitted to the handheld computer. The client-handheld conduit file is received and installed on the handheld computer."* & col.9 line 66 ~ col.10 line 4 *"Referring to FIG. 5E, the installation is initiated by client computer transmitting a query to the handheld computer to determine*

the handheld computer's environment information at step 607. The handheld computer' environment information is stored as the handheld configuration data 424 (FIG. 4) on the handheld computer.")

- storing a second portion of network-specific data at the station that is not accessible by the host computing device (col.6 lines 5-7 *"The memory 310 further preferably includes: communications procedures 314, synchronization procedures 316, authentication procedures 318, a network client 320"* & lines 18-20 *"Authentication procedures 318 are used to authenticate a user's access to the handheld file 224 (FIG. 2) on the installation server 102 (FIG. 1)."*)
- receiving a data block into from the host computing device, wherein the host computing device uses said the device driver to transfer the data block to the station, (col.9 lines 13-20 *"This client-handheld conduit file is an executable file that provides for communication between the client computer and the handheld computer. The installation server receives the request, at step 580, and transmits the client-handheld conduit file to client computer at step 582. The client computer receives the client-handheld conduit file and saves it into its cache as client-handheld conduit file 326 (FIG. 3), at step 584. "*)
- wherein the first portion of network-specific data comprising a plurality of pre-configured network specific parameter that enable the host computer to access the network (col.6 lines 5-7 *"The memory 310 further preferably includes: communications procedures 314, synchronization procedures 316, authentication procedures 318, a network client 320"* & lines 18-20 *"Authentication procedures 318 are used to authenticate a user's access to the handheld file 224 (FIG. 2) on the installation server*

102 (FIG. 1)." & col.12-21 "*Communications procedures 314 are used for communicating with both the network 104 (FIG. 1) and the handheld computer 116 (FIG. 1). ... Authentication procedures 318 are used to authenticate a user's access to the handheld file 224 (FIG. 2) on the installation server 102 (FIG. 1).*" Those communication procedure and authentication procedure may comprise network data to control to access a network.)

- wherein the station controls access to the network by the host computer using the second portion of network-specific data (col.8 lines 42-50 *"To authenticate the user, the network client 320 (FIG. 3) builds an authentication request, which may contain entries for a username and a password, and requests user authentication, at step 554. The user authentication request is received by the installation server at step 552. The installation server authenticates or validates the user, at step 556, by the authentication procedures 216 (FIG. 2) checking the supplied username and password against the user database 226 (FIG. 2).*")

But Bunger do not discloses

- receiving an option for device driver installation, wherein the option is not selectable in the device driver file or in the first portion of network-specific data; installing the sent device driver file based on the received option

However, Fordemwalt discloses

- receiving an option for device driver installation, wherein the option is not selectable in the device driver file or in the first portion of network-specific data; installing the sent

device driver file based on the received option ([0021] "*As part of the installation process, the device driver is configured to self-initialize and invoke an initialization entry point. The initialization entry point may be configured to point to a driver initialization description file which is read by the device driver. The initialization description file includes the name of the peripheral software and an installation method for the peripheral software. This information is utilized by the device driver to install the peripheral software according to the listed installation method.*" Applicant does not define 'an option' in the claim 1. Examiner interpreted it as 'name of the peripheral software'. This information is utilized by the device driver to install the peripheral software.)

- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bunger's teachings by adding receiving an option for device driver installation, wherein the option is not selectable in the device driver file or in the first portion of network-specific data; installing the sent device driver file based on the received option taught by Fordemwalt in order to provide a method includes reading a description file associated with the peripheral in response to an initialization of the device driver during an installation of the device driver on a client computer, and installing the peripheral software on a client computer in response to an installation procedure of the peripheral software included in the description file (see Fordemwalt in paragraph [0011])

Bunger discloses

- wherein the second portion of network-specific data comprises at least one parameter for controlling use of a network by the host computing device (col.8 lines 42-50 "*To*

authenticate the user, the network client 320 (FIG. 3) builds an authentication request, which may contain entries for a username and a password, and requests user authentication, at step 554. The user authentication request is received by the installation server at step 552. The installation server authenticates or validates the user, at step 556, by the authentication procedures 216 (FIG. 2) checking the supplied username and password against the user database 226.")

But both Bunger and Fordemwalt do not disclose

- wherein the at least one parameter sets a length of time that the host computer can access the network once access is granted.

However, Palekar discloses

- wherein the at least one parameter sets a length of time that the host computer can access the network once access is granted (col.7 lines 2-6 "*in the profile 312 of FIG. 3a, the action "Time.sub.-- of.sub.-- day==0900.1700" is an authorization parameter that tells the NAS 66 to determine whether the time of the user's login falls between 0900 and 1700, and if it does not, the NAS 66 is to deny access to the network. This authorization parameter may also be used as a condition for a policy statement as well.*")
- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Bunger's teachings of network-specific data comprises at least one parameter for controlling use of a network by the host computing device by adding at least one parameter sets a length of time that the host computer can access the network once access is granted taught by Palekar in order to provide a policy included

authorization parameter for determining whether a user is authorized access to a resource on the network (col.1 lines 40-43 & lines 57-62)

Per claim 2

Bunger further discloses

- displaying said first portion of network- specific data at the host computing device (col.8 lines 26-30 *"In a preferred embodiment, the events and user interface are a Web-page displaying that the client and/or handheld computer has a particular configuration and can download and install the appropriate file."*)

Per claim 3

Bunger further discloses

- storing an AutoRun file and a Setup file on said station (col.6 lines 64-67 & Fig.4 Memory 410 included component 420; installation procedure is automatically install that implicitly included the autorun file, setup executable to install file).

Per claim 4

Bunger further discloses

- The device driver file is stored at the station in one of a flash memory, a read-only memory, a programmable read-only memory, and a magnetic disk memory (Fig.3 Memory 310 included component 326).

Per claim 5

Bunger further discloses

- The network-specific data define a security configuration and a network configuration (col.6 lines 12-14 & 19-21 & 41-44).

Per claim 7

Bunger further discloses

- The network identifier is an IEEE 802.11 basic service set identifier (col.4 lines 61-65).

5. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over by Bunger, in view of Fordemwalt and Palekar, and further view of Chefalas et al. (US Pub No. 20040015961 A1 hereinafter "Chefalas").

Per claim 6

Bunger discloses

- security configuration comprises authentication-related parameters (col.5 lines 36-38), and wherein said network configuration comprises a network identifier (col.5 lines 16-19; same communication circuitry using on client computer and handheld computer).

But Bunger, Fordemwalt and Palekar do not disclose

- security configuration comprises encryption related parameter.

However, Chefalas discloses

- security configuration comprises encryption related parameter ([0034] e.g. *"Added*

security protection is provided through encryption of the data transmitted between the user's client computer and the server").

- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bunger's teachings by adding security configuration comprises encryption related parameter by Chefalas in order to ensure secrecy and protect communication and in addition encryption can be accomplished through the use of Secure Sockets Layer technology (Chefalas; [0034] lines 11-12).

6. Claims 9, 10, 12, 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Bunger, in view of Robinson et al. (US Pub No. 20050060365 A1 hereinafter "Robinson")

Per claim 9

Bunger discloses

an apparatus comprising:

- A memory for storing at least a device driver file and a first portion of network-specific data, and a second portion of network-specific data (see col.6 lines 5-10 & Fig.3 the memory block 310 which includes client-handheld conduit file).
- a host interface for transferring the device driver file and the first portion of network-specific data (see col.9 lines 28-34 *"After opening the synchronization session, the client-handheld conduit file is transmitted to the handheld computer. The client-handheld conduit file is received and installed on the handheld computer"*).

- a transmitter for transmitting a data block into a network (col.4 lines 56-58 & Fig.1), wherein the data block is received from the host computing device using a device driver represented by the driver file (col.9 lines 13-15 & col.10 lines 12-17);
- wherein the first portion of network-specific data is configured to enable the host computing device to access the network (col.8 lines 26-30 *"In a preferred embodiment, the events and user interface are a Web-page displaying that the client and/or handheld computer has a particular configuration and can download and install the appropriate file."*) and wherein the second portion of network-specific data is unreadable by the host computing device and is configured to control access to the network by the host computing device (col.8 lines 42-50 *"To authenticate the user, the network client 320 (FIG. 3) builds an authentication request, which may contain entries for a username and a password, and requests user authentication, at step 554. The user authentication request is received by the installation server at step 552. The installation server authenticates or validates the user, at step 556, by the authentication procedures 216 (FIG. 2) checking the supplied username and password against the user database 226 (FIG. 2)."*)

But Bunger do not disclose

- And parameters that change over time, wherein the parameters that change over time comprise a signal-strength parameter and a data-rate parameter;

However, Robinson discloses

- And parameters that change over time, wherein the parameters that change over time comprise a signal-strength parameter and a data-rate parameter ([0053] *"Communication*

network context comprises network profile attributes including voice network type, data network type, data transfer speed, gateway type, data packet size, cost(s), security, authentication methods, transfer medium characteristics, for transfer media which may include, e.g., wired, wireless, fiber optic, etc. Additionally, network context may include situational information comprising network stability, bandwidth/data transfer rates, connection quality, transfer latencies, error rates, network load, signal strength, cost, Quality of Service, network protocols, etc")

- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Bunger's teachings by adding parameters that change over time, wherein the parameters that change over time comprise a signal-strength parameter and a data-rate parameter taught by Robinson in order to coordinate and automate information exchange between devices and to select timely, relevant, personalized information that is presented to the user or used for determining the form of presentation to the user ([0010])

Per claim 10

Bunger further discloses

- The network-specific data define a security configuration and a network configuration (col.6 lines 12-14 & 19-21 & 41-44).

Per claim 12

Bunger further discloses

- The network identifier is an IEEE 802.11 basic service set identifier (col.4 lines 61-65).

Per claim 14

Bunger discloses

the apparatus of claim 9 further comprising a host computing device for:

- installing the device driver (col.9 lines 6-15).
- generating the data block (col.10 lines 12-17).
- displaying the first portion of network-specific data (col.8 lines 26-30 *"In a preferred embodiment, the events and user interface are a Web-page displaying that the client and/or handheld computer has a particular configuration and can download and install the appropriate file."*)

Per claim 15

Bunger discloses

- the apparatus of claim 9 wherein the memory is also for storing an AutoRun file and a Setup file (col.6 lines 38-40 & Fig.3 Memory 310 included component 328; installation procedure is automatically install that implicitly included the autorun file, setup executable file).

Per claim 16

Bunger discloses

- the apparatus of claim 9 wherein the memory comprises one of a flash memory, a read-only memory, a programmable read-only memory, and a magnetic disk memory (col.5 lines 20-21).

7. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over by Bunger, in view of Robinson, and further view of Chefalas.

Per claim 11

Bunger discloses

- the method of claim 5 wherein said security configuration comprises authentication-related parameters (col.5 lines 36-38), and wherein said network configuration comprises a network identifier (col.5 lines 16-19; same communication circuitry using on client computer and handheld computer).

But Bunger, Robinson do not disclose

- security configuration comprises encryption related parameter.

However, Chefalas discloses

- security configuration comprises encryption related parameter ([0034] e.g. *"Added security protection is provided through encryption of the data transmitted between the user's client computer and the server"*).
- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bunger's teachings by adding security configuration comprises encryption related parameter by Chefalas in order to ensure secrecy and

protect communication and in addition encryption can be accomplished through the use of Secure Sockets Layer technology (Chefalas; [0034] lines 11-12).

8. Claims 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over by Bunger, and in view of Robinson and further view of Palekar.

Per claim 13

Both Bunger and Robinson do not disclose

- data that sets a length of time that host computer can access the network.

Palekar discloses

- data that sets a length of time that host computer can access the network (col.7 lines 2-6 "*in the profile 312 of FIG. 3a, the action "Time.sub.-- of.sub.-- day==0900.1700" is an authorization parameter that tells the NAS 66 to determine whether the time of the user's login falls between 0900 and 1700, and if it does not, the NAS 66 is to deny access to the network. This authorization parameter may also be used as a condition for a policy statement as well.*")
- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Bunger's teachings of network-specific data comprises at least one parameter for controlling use of a network by the host computing device by adding at least one parameter sets a length of time that the host computer can access the network once access is granted taught by Palekar in order to provide a policy included authorization parameter for determining whether a user is authorized access to a resource on the network (col.1 lines 40-43 & lines 57-62)

9. Claims 17-21 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Bunger, in view of Fordemwalt.

Per claim 17

Bunger discloses

- an apparatus comprising: a transceiver, configured as a network interface card (col.5 lines 15-18 *"The communications circuitry 204 and the communications port 206 preferably include one or more Network Interface Cards (NICs) configured to communicate with the network 104 (FIG. 1) and the client computer 106 (FIG. 1)"*), for: sending a device driver file and a first portion of network-specific data (see col.9 lines 28-34 *"After opening the synchronization session, the client-handheld conduit file is transmitted to the handheld computer. The client-handheld conduit file is received and installed on the handheld computer."* & col.9 line 66 ~ col.10 line 4 *"Referring to FIG. 5E, the installation is initiated by client computer transmitting a query to the handheld computer to determine the handheld computer's environment information at step 607. The handheld computer' environment information is stored as the handheld configuration data 424 (FIG. 4) on the handheld computer."*).
- storing a second portion of network-specific data, the second portion of network data comprising at least one parameter to control access to a network (col.6 lines 5-7 *"The memory 310 further preferably includes: communications procedures 314, synchronization procedures 316, authentication procedures 318, a network client 320"* & lines 18-20 *"Authentication procedures 318 are used to authenticate a user's access to the handheld file 224 (FIG. 2) on the installation server 102 (FIG. 1)."* & col.12-21

"*Communications procedures 314 are used for communicating with both the network 104 (FIG. 1) and the handheld computer 116 (FIG. 1). ... Authentication procedures 318 are used to authenticate a user's access to the handheld file 224 (FIG. 2) on the installation server 102 (FIG. 1).*" Those communication procedure and authentication procedure may comprise network data to control to access a network.)

- transmitting a data block into a network based on the second portion of network-specific data (col.8 lines 53-60 & Fig.5C "*The identification of the user type provides details such as the type of user and handheld files to which the user has access to, or may be interested in, for example, the user's profession or area of speciality. The user type is sent back to the client computer, at step 556, and is received at the client computer at step 558. Based on the user type and whether the user has been authenticated, the client computer then determines, at step 560, if the user is a valid user, i.e., has been authenticated.*")
- a host computing device, comprising a card slot configured for electrically connecting with the network interface card (col.4 lines 61-67 "*In one embodiment, a handheld computer 116 is linked to the client computer 106 via a second communication link 110. ... In one embodiment, the communication link 110 communicates with the handheld computer through a cradle 112. When communicating, the handheld computer 116 rests in the cradle 112.*" In Fig.1, the cradle should have card slot holding for handheld computer and connect to client computer with communication link), the host computing device configured for receiving the device driver file and the first portion of network-specific data (see col.9 lines 28-34 *"After opening the synchronization session, the client-*

handheld conduit file is transmitted to the handheld computer. The client-handheld conduit file is received and installed on the handheld computer." & col.9 line 66 ~ col.10 line 4 "*Referring to FIG. 5E, the installation is initiated by client computer transmitting a query to the handheld computer to determine the handheld computer's environment information at step 607. The handheld computer' environment information is stored as the handheld configuration data 424 (FIG. 4) on the handheld computer.*")

- generating the data block and using the device driver to transfer said data block to the transceiver (col.10 lines 12-17); wherein said first portion of network-specific data is configured to control access by the host computing device to the network (col.8 lines 26-30 *"In a preferred embodiment, the events and user interface are a Web-page displaying that the client and/or handheld computer has a particular configuration and can download and install the appropriate file."*)
- And wherein the host computing device is unable to read the second portion of network-specific data (col.8 lines 42-50 *"To authenticate the user, the network client 320 (FIG. 3) builds an authentication request, which may contain entries for a username and a password, and requests user authentication, at step 554. The user authentication request is received by the installation server at step 552. The installation server authenticates or validates the user, at step 556, by the authentication procedures 216 (FIG. 2) checking the supplied username and password against the user database 226 (FIG. 2)."*)

But Bunger do not discloses

- selecting an option for device driver installation, wherein the option is not selectable in the device driver file or in the first portion of network-specific data; installing a device driver that is represented by the device driver file based on the selected option.

However, Fordemwalt discloses

- selecting an option for device driver installation, wherein the option is not selectable in the device driver file or in the first portion of network-specific data; installing a device driver that is represented by the device driver file based on the selected option ([0021] "*As part of the installation process, the device driver is configured to self-initialize and invoke an initialization entry point. The initialization entry point may be configured to point to a driver initialization description file which is read by the device driver. The initialization description file includes the name of the peripheral software and an installation method for the peripheral software. This information is utilized by the device driver to install the peripheral software according to the listed installation method.*" Applicant does not define 'an option' in the claim 1. Examiner interpreted it as 'name of the peripheral software'. This information is utilized by the device driver to install the peripheral software.)
- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bunger's teachings by adding selecting an option for device driver installation, wherein the option is not selectable in the device driver file or in the first portion of network-specific data; installing a device driver that is represented by the device driver file based on the selected option taught by Fordemwalt in order to provide a method includes reading a description file associated with the peripheral in

response to an initialization of the device driver during an installation of the device driver on a client computer, and installing the peripheral software on a client computer in response to an installation procedure of the peripheral software included in the description file (see Fordemwalt in paragraph [0011])

Per claim 18

Bunger further discloses

- displaying said first portion of network- specific data at the host computing device (col.8 lines 26-30 *"In a preferred embodiment, the events and user interface are a Web-page displaying that the client and/or handheld computer has a particular configuration and can download and install the appropriate file."*)

Per claim 19

Bunger further discloses

- storing an AutoRun file and a Setup file on said station (col.6 lines 64-67 & Fig.4 Memory 410 included component 420; installation procedure is automatically install that implicitly included the autorun file, setup executable to install file).

Per claim 20

Bunger further discloses

- The device driver file is stored at the station in one of a flash memory, a read-only memory, a programmable read-only memory, and a magnetic disk memory (Fig.3 Memory 310 included component 326).

Per claim 21

Bunger further discloses

- The network-specific data define a security configuration and a network configuration (col.6 lines 12-14 & 19-21 & 41-44).

Per claim 23

Bunger further discloses

- The network identifier is an IEEE 802.11 basic service set identifier (col.4 lines 61-65).

10. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over by Bunger, in view of Fordemwalt, and further view of Chefalas.

Per claim 22

Bunger discloses

- wherein said security configuration comprises authentication-related parameters (col.5 lines 36-38), and wherein said network configuration comprises a network identifier (col.5 lines 16-19; same communication circuitry using on client computer and handheld computer).

But Bunger and Fordemwalt do not disclose

- security configuration comprises encryption related parameter.

However, Chefalas discloses

- security configuration comprises encryption related parameter ([0034] e.g. *"Added security protection is provided through encryption of the data transmitted between the user's client computer and the server"*).
- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bunger's teachings by adding security configuration comprises encryption related parameter by Chefalas in order to ensure secrecy and protect communication and in addition encryption can be accomplished through the use of Secure Sockets Layer technology (Chefalas; [0034] lines 11-12).

11. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over by Bunger, and in view of Fordemwalt and further view of Palekar.

Per claim 24

Both Bunger and Fordemwalt does not disclose

- data that sets a length of time that host computer can access the network.

Palekar discloses

- data that sets a length of time that host computer can access the network (col.7 lines 2-6 *"in the profile 312 of FIG. 3a, the action "Time.sub.-- of.sub.-- day==0900.1700" is an authorization parameter that tells the NAS 66 to determine whether the time of the user's login falls between 0900 and 1700, and if it does not, the NAS 66 is to deny access to the*

network. This authorization parameter may also be used as a condition for a policy statement as well.")

- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Bunger's teachings of network-specific data comprises at least one parameter for controlling use of a network by the host computing device by adding at least one parameter sets a length of time that the host computer can access the network once access is granted taught by Palekar in order to provide a policy included authorization parameter for determining whether a user is authorized access to a resource on the network (col.1 lines 40-43 & lines 57-62)

12. Claims 25-29 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Bunger, in view of Fordemwalt, and further view of Maffezzoni et al. (US Patent No. 7,149,978 B1 hereinafter "Maffezzoni")

Per claim 25

Bunger discloses

- A host computing device, comprising:

  means for electrically coupling with a station configured as a host interface card (col.5 lines 15-18 *"The communications circuitry 204 and the communications port 206 preferably include one or more Network Interface Cards (NICs) configured to communicate with the network 104 (FIG. 1) and the client computer 106 (FIG. 1)*")

- means for receiving a device driver file and a first portion of network-specific data from the station (see col.9 lines 28-34 *"After opening the synchronization session, the client-handheld conduit file is transmitted to the handheld computer. The client-handheld conduit file is received and installed on the handheld computer"*)

- wherein the station stores a second portion of network-specific data that is unreadable by the means for receiving (col.8 lines 42-50 *"To authenticate the user, the network client 320 (FIG. 3) builds an authentication request, which may contain entries for a username and a password, and requests user authentication, at step 554. The user authentication request is received by the installation server at step 552. The installation server authenticates or validates the user, at step 556, by the authentication procedures 216 (FIG. 2) checking the supplied username and password against the user database 226 (FIG. 2)."*)

- means for transmitting a data block into a network (col.4 lines 56-58 & Fig.1), wherein the means for receiving generates the data block, wherein the means for receiving uses the device driver to transfer the data block to the station (col.9 lines 13-20 *"This client-handheld conduit file is an executable file that provides for communication between the client computer and the handheld computer. The installation server receives the request, at step 580, and transmits the client-handheld conduit file to client computer at step 582. The client computer receives the client-handheld conduit file and saves it into its cache as client-handheld conduit file 326 (FIG. 3), at step 584. "*), wherein the first portion of network-specific data is configured to enable the means for receiving to access the network (col.8 lines 26-30 *"In a preferred embodiment, the events and user interface are*

a Web-page displaying that the client and/or handheld computer has a particular configuration and can download and install the appropriate file."), and wherein the second portion of network-specific data is configured to control access to the network (col.8 lines 42-50 *"To authenticate the user, the network client 320 (FIG. 3) builds an authentication request, which may contain entries for a username and a password, and requests user authentication, at step 554. The user authentication request is received by the installation server at step 552. The installation server authenticates or validates the user, at step 556, by the authentication procedures 216 (FIG. 2) checking the supplied username and password against the user database 226 (FIG. 2)."*)

But bunger does not disclose

- means for selecting an option for device driver installation, wherein the option is not selectable in the device driver file or in the first portion of network-specific data; means for installing at the means for receiving a device driver that is represented by the device driver file based on the selected option.

However, Fordemwalt discloses

- means for selecting an option for device driver installation, wherein the option is not selectable in the device driver file or in the first portion of network-specific data; means for installing at the means for receiving a device driver that is represented by the device driver file based on the selected option ([0021] *"As part of the installation process, the device driver is configured to self-initialize and invoke an initialization entry point. The initialization entry point may be configured to point to a driver initialization*

description file which is read by the device driver. The initialization description file includes the name of the peripheral software and an installation method for the peripheral software. This information is utilized by the device driver to install the peripheral software according to the listed installation method." Applicant does not define 'an option' in the claim 1. Examiner interpreted it as 'name of the peripheral software'. This information is utilized by the device driver to install the peripheral software.)

- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bunger's teachings by adding means for selecting an option for device driver installation, wherein the option is not selectable in the device driver file or in the first portion of network-specific data; means for installing at the means for receiving a device driver that is represented by the device driver file based on the selected option taught by Fordemwalt in order to provide a method includes reading a description file associated with the peripheral in response to an initialization of the device driver during an installation of the device driver on a client computer, and installing the peripheral software on a client computer in response to an installation procedure of the peripheral software included in the description file (see Fordemwalt in paragraph [0011])

Bunger discloses network-specific data comprising a plurality of pre-configured network-specific parameters, but does not disclose the plurality of pre-configured network-specific parameters comprise parameters for providing status, configuration, diagnostics, and administration

However, Maffezzoni discloses

- the plurality of pre-configured network-specific parameters comprise parameters for providing status, configuration, diagnostics, and administration ([Abstract] "*Icons and graphical user interfaces are displayed providing a plurality of configuration options and diagnostic tools to allow access, evaluation, management* (i.e. administration) *and testing of host adapters and peripheral devices connected thereto in a manner with the look and feel of any other computer system device.*"& col.6 lines 42-46 "*Icons represent various system devices and parameters, and a user selects a particular icon to open a window or screen, another GUI, to access the configuration settings, parameters, and properties for the desired device or system parameter.*")

- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bunger's teachings of network-specific data comprising a plurality of pre-configured network-specific parameters by adding the plurality of pre-configured network-specific parameters comprise parameters for providing status, configuration, diagnostics, and administration taught by Fordemwalt in order to provide a method for allowing access to manage configuration setting of host adapter as well as any peripheral devices connected to the host adapter *and managing the configuration settings of the host adapter by using of the graphical user interface to create configuration changes* (col.3 lines 23-26)

Per claim 26

Bunger further discloses

- comprising means for displaying the first portion of network-specific data at the means for receiving (col.8 lines 26-30 *"In a preferred embodiment, the events and user interface are a Web-page displaying that the client and/or handheld computer has a particular configuration and can download and install the appropriate file."*)

Per claim 27

Bunger further discloses

- comprising means for reading an AutoRun file and for executing a Setup file, wherein the AutoRun file and the Setup file are stored on the station and wherein the Setup file is for installing the device driver at the means for receiving (col.6 lines 64-67 & Fig.4 Memory 410 included component 420; installation procedure is automatically install that implicitly included the autorun file, setup executable to install file).

Per claim 28

Bunger further discloses

- wherein the device driver file is stored at the station in one of a flash memory, a read-only memory, a programmable read-only memory, and a magnetic disk memory (Fig.3 Memory 310 included component 326).

Per claim 29

Bunger further discloses

- wherein the network-specific data define a security configuration and a network configuration (col.6 lines 12-14 & 19-21 & 41-44)

Per claim 31

Bunger further discloses

- wherein the network identifier is an IEEE 802.11 basic service set identifier (col.4 lines 61-65).

13. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over by Bunger, in view of Fordemwalt and Maffezzoni, and further view of Chefalas.

Per claim 30

Bunger discloses

- security configuration comprises authentication-related parameters (col.5 lines 36-38), and wherein said network configuration comprises a network identifier (col.5 lines 16-19; same communication circuitry using on client computer and handheld computer).

But Bunger, Fordemwalt and Maffezzoni do not disclose

- security configuration comprises encryption related parameter.

However, Chefalas discloses

- security configuration comprises encryption related parameter ([0034] e.g. *"Added security protection is provided through encryption of the data transmitted between the user's client computer and the server"*).
- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bunger's teachings by adding security configuration comprises encryption related parameter by Chefalas in order to ensure secrecy and protect communication and in addition encryption can be accomplished through the use of Secure Sockets Layer technology (Chefalas; [0034] lines 11-12).

14. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over by Bunger, and in view of Fordemwalt and Maffezzoni and further view of Palekar.

Per claim 32

Bunger, Fordemwalt and Maffezzoni do not disclose

- data that sets a length of time that host computer can access the network.

Palekar discloses

- data that sets a length of time that host computer can access the network (col.7 lines 2-6 *"in the profile 312 of FIG. 3a, the action "Time.sub.-- of.sub.-- day==0900.1700" is an authorization parameter that tells the NAS 66 to determine whether the time of the user's login falls between 0900 and 1700, and if it does not, the NAS 66 is to deny access to the network. This authorization parameter may also be used as a condition for a policy statement as well."*)

- Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Bunger's teachings of network-specific data comprises at least one parameter for controlling use of a network by the host computing device by adding at least one parameter sets a length of time that the host computer can access the network once access is granted taught by Palekar in order to provide a policy included authorization parameter for determining whether a user is authorized access to a resource on the network (col.1 lines 40-43 & lines 57-62)

Response to Arguments

Applicant's arguments filed on June 19, 2009 have been fully considered but they are not persuasive.

In the remarks, Applicant argues that:

(a) In regard to independent claims 1, 9, 17, and 25 applicant respectfully submits currently amended claims that cited reference does not disclose or suggest.

Examiner's response:

Examiner disagrees.

(a) Applicant's arguments with respect to claims 1, 9, 17, and 25 have been considered but are moot in view of the new ground(s) of rejection - see Fordemwalt, Palekar, Robinson and Maffezzoni, arts made of record, as applied hereto.

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Junchun Wu whose telephone number is 571-270-1250. The examiner can normally be reached on 8:00-17:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wei Zhen can be reached on 571-272-3708. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JW

/Wei Y Zhen/

Supervisory Patent Examiner, Art Unit 2191